Focus on Security

Ausgabe 09, September 2017

SECURITAS

Arbeitsschutz

Secupedia.info befasst sich am 3. August mit der **Fluchtwegsicherung in Arbeitsstätten**. Die Verordnung über Arbeitsstätten setze zusammen mit dem Arbeitsschutzgesetz die EG-Arbeitsstättenrichtlinie 89/654/EWG um. Grundlage für die Normierung der Fluchtwegsicherheit sei die Technische Regel für Arbeitsstätten ASR A2.3. Fluchtwegsicherheit sei gegeben, wenn bei der Ausprägung von Fluchtwegen die Mindestbreite von Fluchtwegen, die baulichen Anforderungen an Fluchtwege, Anforderungen an die Installation in Flucht- und Rettungswegen, eine jederzeit uneingeschränkte Benutzbarkeit, eine Ausprägung der Abschlüsse, die Beschilderung gemäß DIN 4844, Sicherheitsbeleuchtung und die Aufstellung von Flucht- und Rettungswegplänen berücksichtigt seien. Die neuen, in ganz Europa einheitlichen Normen unterschieden Notausgangs- und Paniktürverschlüsse. Der Artikel behandelt insbesondere Notausgangs- und Paniktüren sowie Anforderungen an Fluchttürsysteme.

Betriebshygiene

Sicherheitsberater.de weist am 31. August auf den **SETON Hygieneleitfaden** hin, der über die wichtigsten Hygieneregeln und Standards informiere: Reinigung & Desinfektion, Schädlingsbekämpfung, Schulung und Verhalten der Mitarbeiter sowie Kennzeichnung. Ergänzt werde der Leitfaden um einen Reinigungsplan und eine praktische Hygiene-Checkliste.

Brandmeldeanlage (BMA)

Das Brandschutz Special der Zeitschrift PROTECTOR, Ausgabe August, enthält mehrere Beiträge zum Themenbereich Brandmeldeanlage. Frank Herstix, Honeywell Security and Fire/Novar GmbH, erläutert die **Vorteile modularer BMA** (S. 32/33). Um Zusatzkosten durch Nutzungsänderungen eines Objektes oder Veränderungen in der Risikodefinition durch Sachversicherer vorzubeugen, könne bereits im Vorfeld die BMA in Form eines „Baukastensystems" geplant werden. Eine komplexe BMA, die als modulares System aufgebaut ist, biete Vorteile sowohl für den Planer, den Errichter als auch für den Betreiber des Systems. Natürlich müsse die angebotene Flexibilität für den Errichter überschaubar bleiben, damit das Handling für den Installateur sowie den Betreiber nicht an Komfort verliert. Nachträgliche Erweiterungen könnten durch Hardware- und auch entsprechende Software-Modularität sichergestellt werden. Die Integration von Brandmeldezentralen in ein **vernetztes System** (IoT) wird ebenfalls thematisiert (S. 34/35). So könne im Brandfall die Anzeige auf dem Managementsystem mit allen Informationen erfolgen, die zu diesem Alarm gehören. Zusätzlich könnten Schranken an den Zufahrten angesteuert werden, um Einsatzkräften den ungehinderten Zugang zu ermöglichen. Gleichzeitig übertragene Videoaufnahmen übermitteln in einem solchen Szenario ohne Zeitverzögerung ein exaktes Bild des Vorfalls. Die Vernetzung ermögliche auch den Einsatz von neuen Brandmeldetechniken, wie etwa die videobasierte Branderkennung. Vernetzte Systeme böten Planern und Betreibern ein hohes Maß an Flexibilität. Auch unter Compliance-Aspekten versprächen vernetzte Systeme Effizienzgewinne. Zur Vielzahl neuer Anwendungen im Rahmen des IoT zählten insbesondere Cloud-basierte Remote Services wie etwa Ferndiagnose, Fernparametrierung oder Inbetriebnahme. Der Betrieb der Sicherheitstechnik über eine IT-Infrastruktur unter Einbindung von Cloud-Services biete viele neue Möglichkeiten. Thorsten Teichert, Ei Electronics GmbH, befasst sich mit **vernetzten Rauchwarnmeldern** (S. 36/37). Die Nachfrage nach vernetzten Rauchwarnmeldern habe in den letzten Jahren deutlich

zugenommen. Die Gründe dafür lägen im Bedürfnis nach mehr Sicherheit und mehr barrierefreiem und altersgerechtem Wohnraum. Auch die Integration von Rauchwarnmeldern in Smart-Home-Systeme lasse sich nur mit funkvernetzten Meldern sinnvoll umsetzen. Funkvernetzte Rauchwarnmelder ermöglichten das Abschalten von Stromkreisen im Brandfall. Durch entsprechende Koppelelemente ließen sich Brandschutzschalter über Arbeitsstromauslöser ansteuern. In einer **Marktübersicht** werden 67 Brandmeldesysteme von 29 Anbietern aufgelistet (S. 46/47). 35 Kriterien wurden abgefragt. Verglichen werden Systemaufbau, Möglichkeit eines Zentralen-Netzwerks, die Anzahl der Bedienebenen und die maximale Melderanzahl.

Die Siemens-Division Building Technologies bringe einen neuen Zwischensockel für die **optisch-akustische Brandalarmierung** auf den Markt, meldet sicherheit.info am 1. August. Der Zwischensockel erfülle die speziellen Anforderungen an die optische Alarmierung gemäß der aktuellen europäischen Norm EN 54-23 und biete einen erhöhten Schutz, da im Alarmfall zwei Sinne angesprochen werden. Der loopgespeiste Zwischensockel benötige keine zusätzliche Verkabelung. Er kommuniziere über den Melder-Bus. Aufgrund des eingebauten Isolators im Gerät und der Melder-Looptechnologie werde die Sicherheit gegen Ausfälle erhöht. Bei mehreren installierten Geräten auf dem Melder-Bus sei zudem die Synchronisation von Ton und Blitzleuchte im gesamten Gebäude gewährleistet. EN 54-23-zertifizierte optische Signalgeber eigneten sich insbesondere für Bereiche, die von Menschen mit eingeschränktem Hörvermögen frequentiert werden.

Security insight stellt in der Ausgabe 4-2017, S. 44, das **grafische Informationssystem Aplis** des Brandschutzspezialisten re'graph vor, das Feuerwehren und den Betreibern von Brandmeldeanlagen unmittelbar nach einer Alarmauslösung alle einsatzrelevanten Daten elektronisch zur Verfügung stelle. Damit ermögliche das browserbasierte System eine frühzeitige und wirksame Brandbekämpfung. Aplis bilde ein vollwertiges Feuerwehr-Anzeigetableau ab und zeige meldungsbezogene Feuerwehr-Laufkarten sowie alle im System hinterlegten Brandschutzgrafiken auf Bildschirmarbeitsplätzen an. Eine kostenlose App ermögliche den mobilen Zugriff auf alle Informationen der angeschlossenen Brandmeldezentralen über Tablets und Smartphones. Aplis sei kompatibel zu allen BMA nach DIN 14675 bzw. DIN VDE 0833-1 und -2 und ermögliche damit eine einheitliche und normgerechte Visualisierung von Brandmeldezentralen unabhängig vom Hersteller.

Brandschutz

Nach einer Veröffentlichung von SecuMedia am 24. Juli muss bei allen neu geplanten Gebäuden, unabhängig ob Wohn- oder Zweckbauten, seit Oktober 2016 Überspannungsschutz installiert werden. Grundlage hierfür seien die überarbeiteten Normen DIN VDE 0100-443 und -534 „Errichten von Niederspannungsanlagen". Dabei berücksichtige die novellierte Norm erstmals auch Schaltüberspannungen, die durch Betriebsmittel selbst erzeugt werden. Detaillierte Auskunft über die Neuerungen der Normen und die entsprechenden Pflichten gebe das BHE-Papier „Drastische Änderungen beim Blitz- und Überspannungsschutz".

Mit der **Fluchttürsteuerung in der Elbphilharmonie** befasst sich Security insight in der Ausgabe 4-2017, S. 42/43. Dort sorgten die Systeme von ASSA ABLOY Sicherheitstechnik und der AZS System AG für zuverlässig funktionierende Rettungswege sowie für eine lückenlose Überwachung sämtlicher relevanter Türen. Und das seien stolze 580 Stück, allein 200 in den Flucht- und Rettungswegen. In der Leitstelle liefen die Fäden des Zutrittskontrollsystems Access 3010 auf dem Visu-

alisierungsmodul Process 3010 zusammen. Jede Tür sei elektronisch mit der Leitstelle verbunden. Die Kabel würden innerhalb eines Nutzungsbereichs von einer Tür zur nächsten auf einen sogenannten Strang gelegt, und jeder Strang sei über ein Buskabel direkt mit einem Etagenhauptverteiler verbunden. Von diesen Verteilern liefen die Signale auf zehn Buscontrollern zusammen. Die Struktur sei sehr flexibel. Die Fluchttüren seien modular aufgebaut und flexibel konfigurierbar.

Mehrere Brandschutzthemen werden im Brandschutz Special der Zeitschrift PROTECTOR, Ausgabe August, behandelt. Oliver Eckerle, Hekatron Vertriebs GmbH, befasst sich mit dem rechtssicheren **Rauchschalter-Austausch bei Feststellanlagen** (S. 12/13). Der Austausch gemäß den Fristen aus DIN 14677 gehöre zur normgerechten Instandhaltung. Anlagenbetreiber, die diese Anforderung auf die leichte Schulter nehmen, riskierten im Schadensfall strafrechtliche Konsequenzen, Schadensersatzansprüche und einen Verlust des Versicherungsschutzes. Der Autor geht auf den Stellenwert von DIN-Normen ein. Sie seien keine Rechtsnormen, sondern „private technische Regeln mit Empfehlungscharakter" (BGH). Auch wenn sie nicht mit den anerkannten Regeln der Technik gleichzusetzen sind, sei anerkannt, dass DIN-Normen die Vermutung in sich tragen, den Stand der allgemein anerkannten Regeln der Technik wiederzugeben. Wulf Statz, Vollmer Brandschutzservice GmbH & Co. KG, sieht für die **Kontrolle brandschutztechnischer Einrichtungen** die Unternehmer in der Pflicht (S. 16/17). Der Weg durch den Pflichtendschungel zu „Wartung & Co." sei kompliziert. Der Autor befasst sich mit verschiedenen Arten von Feuerlöschern (einschließlich Kohlendioxid-Feuerlöschern für Serverräume), mit Wandhydrantenanlagen, in den drei Ausführungen nasse oder nass-trockene Wandhydranten und trockene Steigleitungen, mit natürlichen Rauchabzugsanlagen, pneumatischen Anlagen und pyrotechnischen Anlagen. Rainer von zur Mühlen, von zur Mühlen'sche GmbH, thematisiert die **Gefahrenquelle Polystyrol-Schaum** (S. 18/19). Es sei eindeutig falsch, wenn die Bauministerkonferenz feststelle, dass Wärmedämmverbundsysteme (WDVS) mit Polystyroldämmstoffen „ordnungsgemäß zertifiziert und bei der zulassungsentsprechenden Ausführung sicher sind". Bei Dächern sei die heiße Verschweißung der bituminierten Dachpappe die statistisch häufigste Brandursache. Um die Fassaden sicherer zu machen, sei vorgeschrieben, dass alle zwei Etagen „Brandriegel" verbaut werden müssen. Sie unterbrechen die Styropordämmung mit 20 cm breiten Streifen. Dies widerspreche dem Baurecht. Danach betrügen die Mindestabstände von Geschoss zu Geschoss 1,5 m – was sollten da 20 cm bei der Brandlastdichte an der Fassade bewirken? Inzwischen empfehle die Konferenz der Bauminister seit 2015 eine Drei-Meter-Sicherheitszone zu Hausfassaden für brennbare Materialien wie Holz oder Müllcontainer. Stefan Crass, Siemens AG, Building Technologies Division, behandelt die sichere **Ansteuerung von Brandschutzklappen per Feldbus** (S. 20–22). Eine aktuelle Neuentwicklung integriere die Ansteuerung der Brandschutzklappen direkt in den Feldbus der BMA. Zum einen sei damit keine zusätzliche Steuerung notwendig. Zum anderen biete die Lösung alle Vorteile eines EN 54-konformen Peripherienetzwerks auch für die Funktionalität der Brandschutzklappen, ohne dass dafür ein eigenes Leitungsnetz erforderlich wäre. Herkömmlicherweise würden automatische Brandschutzklappen über eine eigenständige Zentrale gesteuert. Durch die Brandschutzklappensteuerung direkt aus der BMZ und damit über das Peripherienetzwerk ergäben sich zahlreiche spezifische Vorteile. Die integrierte Brandschutzklappensteuerzentrale könne die Brandschutzklappen nicht nur in einer einzelnen Anlage, sondern sogar in einem ganzen Anlagenverbund steuern. Gaby Bauer und Sven Kuntschmann, Geze GmbH, zeigen, wie **RWA und Lüftung intelligent kombiniert** werden (S. 26/27). Ob in öffentlichen Gebäuden, Bürobauten oder Schulen

– energieeffizientes Lüften, ein gesundes Raumklima und Brandschutz müssten Hand in Hand gehen. Dazu komme die heute übliche Überwachung der Fensterzustände als zentrale Anforderung in großen Objekten. Es bedürfe der Planung einer sicherheitsgerichteten Lösung in Verbindung mit Gebäudeautomation (KNX), um das Beste aus beiden Welten zu verbinden. Die automatisierten Fenster ermöglichten die direkte Kommunikation mit weiteren Komponenten im KNX-Gebäudesystem, wie zum Beispiel Tastern und Sensoren. Die intelligenten Fensterantriebe unterschieden zwischen Alarm (RWA-) und Lüftungsmodus, das heißt, einer schnellen und maximalen beziehungsweise langsamen, begrenzten und fast geräuschlosen Öffnung.

Cloud Computing

Datenschutzkonformes Cloud Computing für Unternehmen thematisiert der Behörden Spiegel in der August-Ausgabe. 2016 würden bereits zwei Drittel der deutschen Unternehmen Cloud-Lösungen nutzen, wie aus dem Cloud-Monitor des Bitkom hervorgehe. Der Großteil davon beschränke sich jedoch auf eine Private Cloud. Public-Cloud-Lösungen würden nur 29 Prozent der Unternehmen nutzen. Gerade KMU hätten oft nicht die notwendigen technischen, organisatorischen und personellen Ressourcen, um IT-Sicherheit, Datensicherheit und Datenschutz auf hohem Niveau zu gewährleisten. Vorbehalte bestünden vor allem gegenüber großen US-amerikanischen Anbietern. Der EU/US-Privacyshield solle zwar dafür sorgen, dass Daten von EU-Bürgern und -Unternehmen in den USA besonders geschützt sind. Juristisch stehe die Vereinbarung jedoch auf unsicheren Füßen. Die Cloud-Version von Office sowie die Infrastrukturplattform Azure von Microsoft könnten über RZ in Deutschland bezogen werden. T-Systems fungiere als Datentreuhänder. T-Systems verpflichtet sich vertraglich, dass Daten nicht gegenüber Dritten offengelegt werden und kontrolliere ansonsten alle z. B. für Wartungsarbeiten nötigen Zugriffe. Sensible Daten sollten nur in verschlüsselter Form in die Public Cloud gegeben werden. Bdrive von der Bundesdruckerei verschlüssele Daten zunächst direkt beim Anwender und teile die Daten dann in einzelne Fragmente, die redundant bei mehreren verschiedenen Cloud-Speicheranbietern gespeichert würden. Mehrstufige Authentifizierungsmethoden würden sicherstellen, dass nur identifizierte und berechtigte Anwender auf die Daten zugreifen können.

Datenschutz

Die Rechtsanwälte Ingemar Kartheuser und Friedrich Gilsdorf weisen in der FAZ am 16. August auf eine **neue BGH-Entscheidung** mit grundlegenden Aussagen zum Datenschutz hin. Im Breyer-Urteil habe der BGH entschieden, dass IP-Adressen nicht allein deshalb als personenbezogen gelten, weil irgendjemand sie dem Nutzer zuordnen kann. Vielmehr bestehe Personenbezug nur für denjenigen, der tatsächlich selbst über realistische Mittel zur Identifizierung verfüge. Ob Datenschutz greift, wenn ein Unternehmen Autokennzeichen dokumentiert und speichert oder wenn ein IT-Dienstleister zur Wartung auf die verschlüsselte Beschäftigten-Datenbank eines Kunden zugreift oder wenn die Post die Nummern vorgelegter Personalausweise speichert, nicht aber die Namen, werde regelmäßig vom Einzelfall und dort davon abhängen, ob die genannten Unternehmen selbst die erforderliche Verknüpfung zwischen Kfz-Kennzeichen, Personalausweisnummern oder den verschlüsselten Daten und den dahinter stehenden Personen herstellen können. Dass deutsches Datenschutzrecht Seitenbetreibern bisher eine längerfristige Speicherung von personenbezogenen Daten aus Sicherheitsgründen verbietet, stehe im Widerspruch zu der EU-Datenschutzrichtlinie, die eine Zulässigkeit von Datennutzungen auf

Grundlage einer Abwägung der Interessen der datenverarbeitenden Stelle und des Betroffenen ermögliche.

Diebstahl

Wie die FAZ am 25. August meldet, verzeichnet die Deutsche Bahn weniger **Metalldiebstähle**. Im ersten Halbjahr 2017 seien es 220 Fälle gewesen, 119 weniger als im ersten Halbjahr 2016. Der Gesamtschaden sei von 5,6 auf 3,1 Mrd. Euro gesunken. 2.100 Züge seien in diesem Zeitraum stehen geblieben, die Verspätungen hätten sich auf ca. 510 Stunden Verspätungen summiert."

„Mit der **Digitalisierung gegen den Fahrradklau**" titelt die FAZ am 30. August. Das Unternehmen „My Stromer AG" liefere sein neuestes E-Bike Modell ST5 mit einem kleinen, berührungsempfindlichen Bildschirm in der Stange zwischen Sattel und Lenker aus. Dieser sei mit einer SIM-Karte ausgestattet, Das habe den Vorteil, dass immer ein Signal gesendet werde und nicht mit Hilfe des Mobiltelefons und einer Funkstrecke die Daten übertragen werden müssen. Wird das Fahrrad gestohlen, gebe es einen lauten Ton von sich, und es lasse sich dann bequem per Handy orten.

Christina Haberland, Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) stellt in der August-Ausgabe von Veko-online das deutsch-österreichische Verbundprojekt **„AMBOS"** des FKIE und des Austrian Institute of Technology vor, das ein System zur frühzeitigen Erkennung, Meldung und wirksamen Abwehr von Drohnen entwickele. Mittels unterschiedlicher Sensoren (u. a. Funk, Akustik, elektro-optisches Infrarot und Radar) würden Bedrohungen aus dem Luftraum detektiert, die Sensordaten analysiert und zu einem ergonomisch gestalteten Lagebild zusammengesetzt. Dies unterstütze das Sicherheitspersonal bei der Entscheidung aktiver Maßnahmen der Intervention (von der Störung der Funkfernsteuerung oder Bordelektronik bis zum Abfangen mittels eines Netzes).

Der **professionellen Drohnenabwehr** widmen sich mittlerweile einige Dutzend Unternehmen in aller Welt, berichtet die FAZ am 15. August. Zum Aufspüren dienten Radargeräte, Frequenzscanner und Hochleistungsmikrofone. Mit den Sensoren solle sogar der Standort des Piloten ausfindig gemacht werden können. Die Reichweite der Erfassung durch Radiofrequenzsensoren liege bei rund einem Kilometer, hochauflösende Kameras, die als weitere Fahndungstechnik zum Einsatz kommen, erreichten bis zu 250 Meter und Mikrofone rund 70 Meter. Eine Drone Tracker genannte Box mit Infrarotkamera für Nachtaufnahmen, Mikrofonen und Empfänger für Funksignale verkaufe das Kasseler Unternehmen Dedrone für 6.500 Euro. Störsender gegen Drohnen seien in Deutschland allenfalls „behördlichen Bedarfsträgern" erlaubt. Für sie gebe es zwei Möglichkeiten der Störung: zum einen die Unterbindung des Videosignals von der Drohne zum Piloten. Erfolgversprechender sei die Unterbrechung der Steuerbefehle der Fernbedienung. Das System „Smart Responsive Jamming Technology" von Airbus unterbreche die Funkverbindung zwischen Drohne und Pilot, ermittle die Position des Piloten und übernehme die Steuerung der Drohne.

Dokumentenfälschung

Mit dem Thema befasst sich polizei-dein-partner.de. Im Moment seien besonders Banken im Fokus der Dokumentenfälscher. Auch in Baumärkten oder bei Autovermietungen sollten die Mitarbeiter vorgelegte Personalausweise und Führerscheine genauestens überprüfen. Hier würden die gefälschten Dokumente von den Tätern in erster Linie dafür verwendet, sich Kraft- oder Baufahrzeuge

auszuleihen und sie nicht wieder zurückzubringen. In den drei Zeilen der maschinenlesbaren Zone auf der Rückseite des Personalausweises machten Fälscher häufig Fehler. Jede einzelne Ziffer habe eine Bedeutung, und wenn man weiß, wie die Maschine die Zeilen liest, könne man als Dokumentenprüfer auch schnell erkennen, ob die Angaben dort stimmig sind.

Endgeräte

Rechtsanwältin Nina Marcus weist in der FAZ am 9. August darauf hin, dass es für die Einführung von „Bring Your Own Device" (BYOD) einer einvernehmlichen Vereinbarung der Arbeitsvertragsparteien bedarf. Wegen des BDSG müsse der Arbeitgeber sicherstellen, dass auf dem mobilen Endgerät private Daten von dienstbezogenen Daten systematisch getrennt sind, um einen Zugriff des Arbeitgebers auf für ihn unbefugte, private Daten zu verhindern. Dies werde regelmäßig durch die vom IT-Dienst des Unternehmens veranlasste Installation sogenannter Container-Apps gewährleistet. Deren Aufspielen ermögliche gleichzeitig die Fernüberwachung und -sperrung oder auch -löschung unternehmensbezogener Daten. Auf dem Endgerät installierte Apps oder sonstige Software stünden dem Verwender häufig ohne Zahlung eines Entgelts nur zum privaten Gebrauch zur Verfügung.

Mobile Systeme werden als Angriffsziel von Kriminellen immer beliebter, heißt es in der FAZ am 28. August. In den Mobiltelefonen seien auch besonders sensible Informationen wie Bank- oder Gesundheitsdaten gespeichert. Die ließen sich gut verkaufen. Nutzer sollten immer vorsichtig sein, wenn ihre Apps besonders viele Rechte verlangen, also etwa den Zugriff auf die Kontakte oder das Mikrofon und die Kamera. Kriminelle hätten nun ein infiziertes SDK (Software Development Kit) gebaut, das Programmierer und App-Entwickler austrickse und Schadsoftware in ihre Apps integriere. Das Perfide dabei: Mit der Software würden Smartphone-Nutzer in Apps ausspioniert, die auf den ersten Blick nicht verdächtig aussehen. Das sei kein Einzelfall. Anfang August hätten Analysten von Trendmicro 340 Apps im Play Store gefunden, die sogenannte Adware verbreitet haben.

Einzahlungstresor

Prosegur stellt Banken Einzahlungsautomaten zur Verfügung, berichtet Security insight in der Ausgabe 4-2017, S. 28/29. Im Detail würden Hardware, Applikation und Prozesse bereitgestellt, die Systeme auf Füllmengen, Versicherungslimits sowie mögliche Störungen überwachen. Dabei gewährleiste der Dienstleister den technischen Service von „First and Second Line Maintenance-Rufbereitschaft". Zum Cash Management und SB-Geräteservice gehörten auch die Analyse der Geldströme in den Geräten und das Monitoring bzw. Reporting. Die Vorteile des Systems: Entkopplung des Bargeldprozesses vom Filialprozess; mehr Effizienz im Bargeldhandling durch Prozessautomatisierung; Entlastung der Notenrecycler; optimaler Versicherungsschutz.

Evakuierung

Dr. Laura Künzer, Dipl.-Psych., und Christian Spielvogel, Kreisbrandmeister, befassen sich in einem Brandschutz Special der Zeitschrift PROTECTOR, August 2017, S. 6–8, mit dem **Verhalten von Menschen im Brandrauch.** Psychologische Gründe seien dafür maßgebend, dass Menschen im Brandrauch verbleiben oder durch den Rauch gehen: Neugier oder Gewohnheiten spielten dabei ebenso eine Rolle wie mangelndes Wissen über die verheerende Giftigkeit des Rauchs und fehlende Informationen. Als Rettungswege würden vor allem bekannte Wege genutzt.

In Ausnahmesituationen verstärke sich auch das Bedürfnis, mit anderen Menschen zusammen zu bleiben. Das führe auch zu einer höheren Bereitschaft, sich führen zu lassen. Die Entscheidung, einen verrauchten Bereich zu verlassen oder in ihm zu bleiben, werde beeinflusst durch die persönliche Einschätzung der Gefährdung sowie Wissen, Erfahrung und Verarbeitung von aktuellen Informationen.

Martin Grell, Gesellschaft für Sicherheitstechnik mbH, befasst sich im Brandschutz Special der Zeitschrift PROTECTOR vom August 2017, S. 28/29, mit dem **Missbrauch von Türen in Fluchtwegen**. Die 2015 veröffentlichte EN 13637 „Elektrisch gesteuerte Fluchttüranlagen für Türen in Fluchtwegen" eröffne neue Lösungsansätze gegen diesen Missbrauch. Die Norm setze auf dem Systemgedanken auf (Verriegelungs-, Steuerungs- und Auslöseelement), schreibe den SIL2 Sicherheitsstandard fest und umfasse eine Vandalismusprüfung. Der Klassifikationsschlüssel sehe Dauerfunktionstests von bis zu einer Mio. Zyklen vor. In Fällen, in denen die nach EltVTR zugelassene elektrische Türverriegelung keine ausreichend hohe Hemmschwelle biete, bedürfe es einer Zustimmung im Einzelfall, um die Hemmschwelle durch Zeitverzug oder Weglassen des Nottasters zu erhöhen.

PROTECTOR enthält im Brandschutz Special vom August 2017, S. 44/45, eine **Marktübersicht** über **33 Fluchtwegsicherungssysteme** von 15 Anbietern mit den Kriterien Zulassungen, Montage, Stromversorgung, Eignung für Zylinderprofile, optische und akustische Signalisierung.

Katharina Meedt, Heinrich Strunz GmbH, behandelt im Brandschutz Special, Ausgabe August 2017, S. 23, die Sicherung von Flucht- und Rettungswegen durch **Rauchschutzdruckanlagen** (RDA), die die Ausbreitung von Rauch umgehend zuverlässig verhindern. Sicherheitstreppenräume müssten so beschaffen sein, dass Feuer und Rauch nicht in sie eindringen können. Um dies zu erreichen, werde zwischen dem Sicherheitstreppenraum und den umgebenen Nutzungseinheiten eine kontrollierte positive Druckdifferenz erzeugt. Die RDA-Anlage müsse über Rauchmelder automatisch ausgelöst werden können.

Gebäudesicherheit

Sicherheit.info stellt am 11. August das **Interface KNX 400 IP** (Feldbus zur Gebäudeautomation) von Telenot vor, das Gebäudeautomation nach KNX-Standards mit professioneller Sicherheitstechnik verknüpfe. Es agiere als Kommunikationsmodul zwischen der EMA und der KNX-Steuerung im Gebäude. So senke sich auf Wunsch des Anwenders etwa automatisch die Heizungstemperatur beim Scharfschalten der Alarmanlage, im Einbruchsfall gehe die gesamte Beleuchtung an und wenn es brennt, würden die Rollläden hochfahren. Nach VdS und DIN 51031 zertifizierte Einbruchmelder „aus der Telenot-Alarmwelt" könnten dank des Interface KNX 400 IP als Aktoren für die Gebäudeautomation verwendet werden. Das spare Komponenten und ermögliche ein objektspezifisches Rundumkonzept aus Steuern, Überwachen und Schützen des Gebäudes nach strengsten Sicherheitsstandards. Zu diesen Standards gehöre die Sabotageüberwachung der Systemkomponenten vor mechanischer oder elektronischer Fremdbeeinflussung, die Leitungs- und Funkstreckenüberwachung zu allen Sicherheitskomponenten. Ebenso sei die sichere optische und akustische Alarmierung vor Ort, wie auch die stille Alarmübertragung an Dritte via IP und GSM-Funkersatzweg, für die Sicherheit von elementarer Bedeutung. Die Bedienung könne über ein Telenot-Touch oder Funkbedienteil im Gebäude erfolgen oder über eine KNX-Steuereinheit. Möglich sei dies ebenso per Alarmanlagen-App „Buildsec" überall und jederzeit vom Smartphone oder Tablet aus. Bei dieser Verbindung

komme eine hochsichere Verschlüsselung zum Einsatz, die auch Banken zur Datenübertragung nutzen.

Gefahrenmanagement-system

Mit einem einheitlichen Gefahrenmanagementsystem im Industriebetrieb befasst sich Security insight in der Ausgabe 4-2017, S. 20/21. Um die Zusammenarbeit mit unterschiedlichen Herstellern technischer Sicherheitsanlagen zu ermöglichen, biete Winguard von Advancis ein herstellerneutrales Gefahrenmanagementsystem, das die gesamte Infrastruktur eines Standortes integriert. Die vorhandenen Kommunikations- und Einsatzleitsysteme würden angebunden. Vorteile des einheitlichen Managementsystems seien die Integration aller technischen Subsysteme, eine einheitliche Bedienung aller technischen Anlagen, Redundanzkonzepte, Visualisierung von Störmeldungen, Automatisierung von Ab- und Zuschaltungen von Meldern in verschiedenen Betrieben, Überwachung der IT-Infrastruktur, rechtssichere Dokumentation und organisatorische Einbindung in übergreifende Sicherheitskonzepte.

Gefahrstoffe

Zertifizierte Brandschutzlager für Gefahrstoffe werden im Brandschutz Special der Zeitschrift PROTECTOR, August 2017, S. 40, behandelt. Teil der Zulassung des Deutschen Instituts für Bautechnik (DIBt) sei auf der einen Seite die Konstruktion des Lagersystems, die verbaute Auffangwanne auf der anderen Seite. Für die allgemeine bauaufsichtliche Zulassung müsse nachgewiesen werden, dass ein Bauwerk durch witterungsbedingte Lasten keinen Schaden nimmt, und dass austretende Flüssigkeiten sicher aufgefangen werden. Die genormten Vorgaben müssten durch reale Brandversuche überprüft werden. Dabei müsse die Konstruktion extremen Bedingungen mindestens 90 Minuten lang wiederstehen.

Geldautomatensicherheit

Wie die FAZ am 26. August meldet, ist nach Jahren eines rasanten Anstiegs die Zahl der gesprengten Geldautomaten in Deutschland in diesem Jahr bislang erstmals wieder leicht rückläufig. Wie das BKA auf Anfrage mitteilte, wurden im ersten Halbjahr 2017 in Deutschland 140 Geldautomaten gesprengt. Das seien 40 Automaten oder gut 20 Prozent weniger als im gleichen Vorjahreszeitraum. Die Zahl dieser Delikte sei bis zum vorigen Jahr immer weiter gestiegen, von etwa 45 Fällen 2012 über 157 Fälle 2015 bis auf 318 Fälle 2016.

Michael Salat, Avast, beschreibt am 31. Juli in security-insider.de, wie **Geldautomaten mit Malware ausgeraubt** werden. Eine neue Angriffsmethode infiziere Geldautomaten mit Malware und lasse sie das Bargeld auf Kommando ausgeben. Die Angriffe durch Malware ersetzten zunehmend klassischen Geldautomatenbetrug (Skimming), da so ein fast gefahrloser Bankraub möglich werde. Einer der neuesten Angriffe dieser Art sei eine Masseninfektion russischer Geldautomaten über das interne Netzwerk eines Geldinstituts gewesen. Interessant sei die Verwendung einer dateilosen Malware, die im Speicher des Rechners ausgeführt wird und immun ist gegen einen Betriebssystem-Neustart des infizierten Geldautomaten, das üblicherweise auf Windows basiere.

IT-Sicherheit

Peter Marwan weist auf silicon.de am 31. Juli darauf hin, dass das Testlabor AV-Comparatives 15 kostenlose **Antivirus-Produkte** untersucht und vor allem Unterschiede zu den Bezahlvarianten ermittelt habe. Überprüft worden seien unter anderem Angebote von Avast, Avira, Bitdefender, Comodo, Kaspersky, McAfee, Microsoft, Panda, Sophos und ZoneAlarm. Kaspersky habe für Oktober 2017 eine kostenlose Version der Antiviren-Software aus seinem Haus angekündigt („Kaspersky Free"). Bei den Gratisangeboten von Bitdefender, MacAfee und Panda seien die wesentlichen Funktionen tendenziell einfacher gehalten als in der Bezahlvariante, was für wenig versierte Nutzer sogar ein Vorteil sein könne. Mehr Funktionen müssten nicht zwangsläufig auch einen besseren Schutz bedeuten. Für den Einsatz in Unternehmen seien kostenpflichtige Versionen aber schon deshalb meist besser geeignet, weil nur sie die zentrale Verwaltung und Kontrolle erlauben.

SecuMedia befasst sich am 21./23. Juli mit der **Malware-Kampagne „Stantinko"**, die infizierte Systeme zu einem Botnet hinzufüge. Mehr als eine halbe Mio. Nutzer seien betroffen. Die Malware sei komplex und extrem anpassungsfähig. So habe es „Stantinko" geschafft, über fünf Jahre lang unentdeckt zu agieren und ein Botnet von mehr als 500.000 infizierten Systemen zu bilden. Das sei das Ergebnis einer umfassenden Untersuchung des Security-Softwareherstellers ESET. Die meisten Betroffenen haben ESET in Russland und in der Ukraine entdeckt. Stantinko infiziere Systeme über Filesharing-Webseiten und locke Nutzer mit kostenloser Software. Der Infektionsvektor installiere eine Reihe auffälliger Anwendungen. Gleichzeitig werde das Schadprogramm unauffällig im Hintergrund installiert. Zugangsdaten zu kompromittierten Accounts würden auf dem Schwarzmarkt verkauft.

SecuMedia sieht nach einem Bericht vom 21. Juli eine weiterhin hohe **Bedrohung für Android-Geräte**. Alle elf Sekunden würden Analysten eine neue Android-Schad-App entdecken. Das seien über 333 pro Stunde. Im ersten Halbjahr 2017 hätten die G DATA Sicherheitsexperten 1,5 Mio. Android-Schaddateien gezählt. Die Bedrohung bleibe hoch. Derzeit schienen Cyberkriminelle ihre Malware-Kampagnen etabliert zu haben und auf andere Methoden als Datendiebstahl zu setzen. Für das Gesamtjahr 2017 rechneten die G DATA Experten mit rund 3,5 Mio. neuen Android-Schad-Apps.

Im Interview in Security Insight (Ausgabe 4-2017, S. 10–12) nimmt MdB Stephan Mayer zur Notwendigkeit einer weiteren **Novellierung des IT-Sicherheitsgesetzes** Stellung. Falschmeldungen, die in sozialen Netzwerken mit falschen Zitaten von Politikern oder Mandatsträgern unterlegt werden, könnten mit dem bisherigen Strafrecht nicht ausreichend geahndet werden. Der Anwendungsbereich des IT-Sicherheitsgesetzes müsse zudem um den Chemiebereich und die Rüstungsbranche erweitert werden. Der innenpolitische Sprecher der CDU/CSU-Bundestagsfraktion äußert in dem Interview die Überzeugung, dass die privaten Sicherheitsdienstleister eine wichtige Säule in der Sicherheitsarchitektur Deutschlands darstellen.

Wie silicon.de am 9. August berichtet, hat Microsoft unter anderem zwei als kritisch eingestufte Sicherheitslücken geschlossen, die in allen unterstützten **Windows**-Versionen stecken. Ein Angreifer könne demnach aus der Ferne Schadcode einschleusen und ausführen und so die vollständige Kontrolle über ein System übernehmen. Laut Microsoft konnte ein Angreifer auf diese Art Programme installieren, Daten einsehen, ändern oder löschen oder ganz neue Benutzerkonten mit vollständigen Rechten anlegen. Einer der beiden kritischen Fehler werde durch die Windows-Suche ausgelöst. Er lasse sich mit Hilfe speziell gestalteter Nachrichten aus-

nutzen, die an den Windows-Suchdienst geschickt werden. In einem Enterprise-Szenario solle es sogar möglich sein, die Schwachstelle über eine SMB-Verbindung auszunutzen und so die Kontrolle über einen Zielcomputer zu übernehmen. Trend Micro halte in dem Zusammenhang sogar einen Exploit für möglich, der die Verbreitung eines Wurms erlaubt.

Sabrina Storrer Jenni, Legic Identsystems AG, behandelt in der Ausgabe 7/8-2017, S. 33, der Zeitschrift PROTECTOR **Sicherheitsrisiken bei mobilen ID-Lösungen in Hotels**. Dass der Chaos Computer Club im Dezember 2016 den Hack eines Türschlosses und der zugehörigen mobilen App verkündete, welche mittels Bluetooth Low Energy mit dem Schloss kommuniziert, könne möglicherweise Konsequenzen für Hotels haben, in denen mobile Zimmerschlüssel zum Einsatz kommen. Legic biete End-to-End-Systeme an, die ein Hacken von mobilen ID-Lösungen verhindern können. Hierbei würden ein Leser-IC mit Bankenlevel (EAL 5+) zertifiziertem, manipulationssicherem Secure-Element im Schloss und ein Hardware-Security-Modul im cloudbasierten Trusted-Service zum Einsatz kommen. Das von Legic eingesetzte Secure-Element biete eine sichere Umgebung für das Speichern von Schlüsseln, kryptografischen Berechnungen und für die Speicherung essentieller Software für Sicherheit und Geschäftsbelange.

Rainer Giedat, Nside Attack Logic GmbH, befasst sich in der Ausgabe 7/8-2017, S. 57, der Zeitschrift PROTECTOR mit „**vernetzter Unsicherheit".** Die vollständige Vernetzung aller Geräte des „Internet of Things" und aller Systeme einer voll vernetzten Produktion mit Industrie 4.0 auf der einen Seite und eine Segmentierung der Netze auf der anderen scheinen sich auszuschließen. Auf den zweiten Blick werde jedoch klar, dass die Trennung bei geeignet gesetzten und gesicherten Übergängen zum Informationsaustausch zwischen den Netzen größtenteils aufrecht erhalten bleiben kann.

Auf die Frage „Was tun gegen Internetkriminalität?" geben Experten in dem Verlagsspezial „**IT für den Mittelstand"** der FAZ vom 10. August Antworten. Nach Christian Ehlen, Twinsec, ist in mittelständischen Unternehmen Risikokompetenz vorhanden. „Was hier fehlt, ist das Vermögen, Angriffen gezielt entgegenzuwirken oder diese nach kurzer Zeit zu erkennen und zu kontrollieren." Die Folge sei eine Asymmetrie zwischen denjenigen, die mit einer Sicherheitsarchitektur das Unternehmen schützen, und denen, die über die Ausnutzung weniger Schwachstellen diese Architektur zu Fall bringen können. „Die Problemstellung besteht für die Unternehmen darin, dass sämtliche Identitäten über den kompletten Aktionsradius einschließlich der Geschäftspartner, Cloud-Dienste und Kunden eindeutig sind", schildert Andreas Martin, First Attribute AG. Nur unter dieser Voraussetzung greife der zweite Schritt, die Zugriffskontrolle, umfassend und verlässlich. Mittelständler könnten intern oft nicht auf die Ressourcen zugreifen, um sich hinreichend vor Angriffen aus dem Cyberspace und von innen zu schützen. Um die sicherheitsrelevanten Aufgaben dennoch zu bewältigen, empfiehlt Philipp Kleinmanns, Materna, über das Vorgehensmodell ISIS12 ein Informations-Sicherheitsmanagementsystem herauszubilden. Harald Reisinger, Radar Services, fordert die Unternehmen auf, eine saubere Analysestruktur zu implementieren, um Schwachstellen in Prorammen sowie abnormen Verhaltensweisen in IT-Systemen und verdächtigen Datenströmen auf Verbindungen auf die Spur zu kommen. Er plädiert in diesem Zusammenhang für den Einsatz von IT Security Monitoring als Frühwarnsystem.

Das finnische Unternehmen F-Secure betreibe weltweit 37 „Honeypots", die pro Jahr 330 Mio. Angriffen ausgesetzt seien, berichtet die FAZ am 19. August. In Deutschland stünden drei davon, auf die 25 Mio. Angriffe pro Jahr erfolgten. Sie zeigten auch die Herkunft von Cyberangriffen. Nach dem Ende Juli veröffentlichten „**Trendreport Cyberattacken"**

seien 38,6 Prozent der 11,3 Mio. Angriffe im 2. Quartal 2017 aus Russland erfolgt, gefolgt von Deutschland selbst mit 31,3 Prozent und 21,6 Prozent aus Amerika. Man könne aber nicht sagen, ob die Angriffe tatsächlich ihren Ursprung in den aufgeführten Ländern haben, denn Hacker könnten ihre Ziele über eine Kette verschlüsselter Server angreifen. Deutschland werde weiter ein beliebtes Ziel von Hackerangriffen bleiben, auch weil es etwa gegenüber Skandinavien technisch im Rückstand sei.

Deutsche fordern mehr Sicherheit im Netz, titelt die FAZ am 19. August. Dabei sei die von Dimap realisierte Untersuchung des Deutschen Instituts für Vertrauen und Sicherheit im Internet (Divse) geprägt von „auffallenden Paradoxien". Zum einen stimmten 83 Prozent der Internetnutzer der Aussage zu, dass jeder Anwender selbst für seine Sicherheit im Internet verantwortlich ist. Gleichzeitig bezweifele die Mehrheit von 57 Prozent, dass der Einzelne dieser Verantwortung überhaupt gerecht werden kann. 85 Prozent der Befragten verlangten, dass sich der Staat stärker um Sicherheit im Internet kümmert. Gleichzeitig trauen jedoch 84 Prozent dem Staat nicht zu, dass er dieser Aufgabe gerecht werden kann. 84 Prozent der Internetnutzer erwarteten auch von Unternehmen die Übernahme von Verantwortung. Und zwei Drittel hätten nur geringes Vertrauen, dass diese sich ausreichend um die Sicherheit ihrer Kunden kümmern. Die globalen Ausgaben für Produkte und Dienstleistungen in Informationssicherheit würden nach einer Prognose des Analysehauses Gartner 2017 auf 86,4 Mrd. Dollar ansteigen, sieben Prozent mehr im Vergleich zu 2016.

Es gebe fünf Gebiete, auf denen **Cyberversicherungen** sinnvoll seien, meint KPMG (FAZ vom 30. August): Identitätsdiebstahl, Betrug im Zahlungsverkehr, Anschläge auf Hard- und Software und Betriebsunterbrechungen durch Cyberkriminalität. Hinzu kämen Schäden bei Dritten, in denen es um eine Art Cyber-Haftpflichtversicherung gehe. Die Prämien hingen unter anderem von der Unternehmensgröße ab. Als Unternehmen mit zwei bis drei Mio. Euro Umsatz im Jahr zahle man etwa 1.500 Euro im Jahr. Das Marktvolumen für Cyberversicherungen in aller Welt werde auf 4 bis 4,5 Mrd. Dollar jährlich geschätzt. Die Cyberversicherungen sicherten weder alle denkbaren Cyberrisiken ab, noch gebe es eine Deckung in unbegrenzter Höhe.

IuK-Kriminalität

Mit der **virtuellen Verletzbarkeit von Seefahrtschiffen** befasst sich Security insight in der Ausgabe 4-2017, S. 18/19. Containerschiffe seien heute schwimmende Rechenzentren, die zahlreiche Angriffspunkte für Freibeuter im Cyberraum böten. Das BSI äußere sich in einem Magazin: „Die Zeit ist reif für Cyber Security an Bord von Schiffen." Wissenschaftler der Sicherheitsfirma Trend Micro hätten zum Beispiel ein Sicherheitsleck in einem Funksystem enthüllt, das weltweit von über 400.000 Schiffen eingesetzt wird. Problemlos hätten die IT-Spezialisten des Unternehmens Schiffe auf dem Radar verschwinden lassen, Routen manipulieren oder falsche Notrufe absetzen können. Alleine die Flut von E-Mails, die zwischen den Schiffen und den Reedereien hin und her schwappe, sei allein schon ein Einfallstor für Malware. Die International Maritime Organization fordere, dass Reedereien dringend eine Anweisung für die Mitglieder der Schiffscrew benötigen, wie sie mit sozialen Medien im Internet umgehen sollen.

Die FAZ befasst sich am 17. August mit dem Hackerangriff mittels des Computervirus „NotPetya" am 27. Juni, von dem Hunderte Unternehmen betroffen waren. Der Virus habe sich auch durch die Systeme des Schifffahrts- und Ölkonzerns Maersk gefressen und erhebliche Störungen verursacht. Container-

frachter seien auf offener See stehengeblieben. Hafenkräne haben keine Boxen mehr verladen können. Selbst die interne Kommunikation in der Kopenhagener Zentrale sei zeitweise lahmgelegt gewesen. Die Attacke habe Maersk eine Menge Geld gekostet. Wie der Konzern berichte, dürfte das Ergebnis im dritten Quartal durch die Attacke mit 200 bis 300 Mio. Dollar belastet werden. Die Reederei und APM Terminals verzeichneten Umsatzausfälle, zudem schlügen hohe Kosten für die Wiederherstellung der Systeme zu Buche.

Mit statistischen Angaben erläutert der Behörden Spiegel in der August-Ausgabe, dass der Cyberraum mit der fortschreitenden Digitalisierung für kriminelle Akteure immer attraktiver wird: Die Anzahl der öffentlich bekannt gewordenen **Software-Sicherheitslücken** habe von 7.217 im Jahr 2011 bis 2016 auf 10.197 zugenommen. Bundesweit erfasste Straftaten mit Handlungsort in Deutschland wurden 2015 insgesamt 45.793, 2016 einschließlich Computerbetrug 82.649 erfasst. Durch Cyberkriminalität sind Unternehmen in den letzten zwei Jahren Gesamtschäden in folgenden Schadensklassen entstanden: neun Prozent unter 10.000 Euro, 33 Prozent 10.000–99.999 Euro, 17 Prozent 100.000–999.999 Euro, fünf Prozent über eine Mio. Euro. Weltweit zahlen 34 Prozent der Unternehmen Lösegeld bei Ransom-Angriffen. In Deutschland sind es 16 Prozent.

Stefan Beiersmann berichtet in silicon.de am 14. August, dass Forscher von FireEye eine Hacking Kampagne aufgedeckt hätten, bei der versucht werde, aus der Ferne Anmeldedaten von Nutzern zu stehlen, die **WLAN-Netzwerke in Hotels** verwenden. Dabei komme der Windows-Exploit zum Einsatz, den Hacker auch für die Verbreitung der Ransomware WannaCry sowie Petya/NotPetya benutzt haben. Betroffen seien derzeit vor allem Hotels in Europa. FireEye betone, dass öffentliche WLAN-Netze eine erhebliche Bedrohung darstellen. Sie seien „wann immer möglich zu meiden". E-Mails mit einem schädlichen Dokument mit dem Titel „Hotel_Reservation_form.doc solle Mitarbeiter der Unternehmen dazu verleiten, ein Makro auszuführen, das wiederum die für AÖPT28 typische Malware GameFish einschleuse. Auch wenn sich die Angriffe jeweils gegen das vollständige Netzwerk eines Hotels richten, gehe FireEye davon aus, dass es die Täter auf einzelne Gäste abgesehen haben, beispielsweise auf Geschäftsleute oder Regierungsvertreter, die in den Hotels absteigen.

Martin Schindler berichtet in silicon.de am 11. August, die **Ransomware Mamba** sei wieder da. Bereits Ende vergangenen Jahres hatte die gefährliche Verschlüsselungssoftware großen Schaden angerichtet. Die Besonderheit des Erpresserschadprogramms sei, dass es nicht nur einzelne Dateien verschlüsselt, sondern die gesamte Festplatte sperrt. Kaspersky Labs melde nun in einem Blog, dass die Organisation, die hinter diesem Schädling stehe, offenbar die Arbeit wieder aufgenommen habe. Die Angriffe richteten sich ausschließlich an Unternehmen. Derzeit sei völlig unklar, wer hinter der Attacke steht.

Jüngste Vorfälle unter den Stichworten „Wannacry" und „Nyetya" zeigen nach einem Bericht in der FAZ am 25. August die schnelle Verbreitung und breite Wirkung von Angriffen, die wie traditionelle Erpressersoftware (Ransomware) aussehen, aber viel zerstörerischer seien. Die Angreifer zielten zunehmend auf die Zerstörung von Sicherheitskopien und anderen Sicherheitsnetzen von Unternehmen ab, was eine Wiederherstellung von Daten nach einem Angriff verhindern solle. Zu den neuen Angriffs-, Verschleierungs- und Umgehungstechniken gehörten „**Destruction of Service"-Angriffe (DeOS):** Diese könnten Backups und Sicherheitsnetze von Unternehmen zerstören, die zur Wiederherstellung von Systemen und Daten nach einem Angriff erforderlich sind. Erfolgreiche Angriffe dieser Art seien sehr schädlich, da Unternehmen keine Möglichkeit der Wiederherstellung bleibe. Hinzu komme „dateilose Malware".

Das sei eine Software, die nicht auf der Festplatte, sondern nur im flüchtigen Speicher vorliege. Sie lasse sich schwerer erkennen oder untersuchen, da ein Neustart die Malware zunächst lösche. Zudem würden anonymisierte und dezentrale Infrastrukturen genutzt wie zum Beispiel Tor, um die Kommando- und Kontrolltätigkeiten zu verschleiern. Hinzu kämen noch „**Business E-Mail Compromise"-Angriffe (BEC).** Die Art von Angriffen verleite Mitarbeiter dazu, über eine offiziell aussehende E-Mail Überweisungen an die Angreifer auszuführen. Zwischen Oktober 2013 und Dezember 2016 seien mit BEC-Angriffen insgesamt 5,3 Mrd. Dollar gestohlen worden. Für die Wirksamkeit von Sicherheitspraktiken sei die Zeit bis zur Erkennung, also dem Zeitfenster zwischen einem Angriff und dem Erkennen einer Bedrohung, eine entscheidende Kenngröße. Sie zu verkürzen bedeute, den Aktionsraum der Angreifer zu begrenzen und Schäden zu minimieren.

Wie Peter Marwan auf silicon.de am 21. August berichtet, hat das SANS Institute, eine kooperative Forschungs- und Ausbildungsorganisation, die Ergebnisse einer im Mai und Juni durchgeführten **Umfrage zur IT-Bedrohungslage** vorgelegt. Die dafür weltweit befragten 263 Sicherheits- und IT-Experten kämpften demnach vor allem mit Phishing sowie den spezialisierten Varianten „Spearphishing" und „Whaling". 72 Prozent hätten eine dieser Angriffsformen als Problem benannt. Sie lägen damit deutlich vor Spyware (50 Prozent) und Ransomware (49 Prozent) sowie Trojanern (47 Prozent). Den größten Schaden richteten den Befragten zufolge aber die Phishing-Techniken, Ransomware und DDoS-Attacken an.

Die Zahl der **Angriffe auf cloudbasierte Microsoft-Konten** sei innerhalb eines Jahres (erstes Quartal 2016 bis erstes Quartal 2017) um 300 Prozent gestiegen, berichtet heise.de am 22. August. Das gehe aus Microsofts aktuellem Security Intelligence Report hervor. Erfolgreiche Kompromittierungen resultierten meist aus der Nutzung schwacher, leicht zu erratender Passwörter und deren schlechter Verwaltung.

Krisenregionen

Türkei-Krise verunsichert Geschäftsreisende, titelt die FAZ am 9. August. In deutschen Unternehmen wachse die Verunsicherung, ob Mitarbeiter noch auf Geschäftsreisen in die Türkei geschickt werden können. Der VDR, Zusammenschluss von Geschäftsreiseverantwortlichen aus der deutschen Wirtschaft, rate zwar nicht zum Verzicht auf Reisen, mahne aber zur Vorsicht. Geschäftsreisenden, die nicht nur für einzelne Tage in die Türkei fahren, sei zu empfehlen, sich in die Krisenvorsorgeliste des Auswärtigen Amtes einzutragen. Den Überblick zu behalten, wo sich Geschäftsreisende befinden, sei ohne technische Lösungen schwer. Immer mehr Unternehmen nutzten Traveller-Trackingsysteme, um Reiseabläufe nachvollziehen zu können.

Ladungsdiebstahl

Über **„Planenschlitzer und Dieseldiebe"** berichtet die FAZ am 4. August. Eine Statistik des hessischen LKA führe Ladungsdiebstähle auf. Ihre Zahl sei in Hessen 2016 im Vergleich zum Vorjahr von 110 auf 306 Fälle gestiegen. Anhand von Daten einzelner LKÄ gingen die Autoren eines Berichts des BAG vom Februar 2017 von einer Fallzahl in Deutschland „im hohen vierstelligen Bereich" aus. Die Versicherungsbranche schätze den jährlichen Schaden durch Ladungsdiebstähle auf 300 Mio. Euro. Weil Häuser und Wohnungen immer besser gesichert seien, verlegten sich nun mehr Kriminelle auf LKA. Bei der Wahl ihrer Beute seien die Diebe wählerisch. Sie arbeiteten oft regelrecht auf Auftrag und suchten nach bestimmten Waren. Oft

seien es organisierte Banden. In Einzelfällen bedienten sie sich sogar eigens gegründeter Scheinfirmen oder kauften insolvente Speditionsunternehmen auf, um über Online-Frachtbörsen in betrügerischer Absicht an Aufträge zu kommen. Überdurchschnittlich oft kämen die Täter aus osteuropäischen Ländern. Bevorzugt würden sie auf ungesicherten Parkplätzen zuschlagen. Die Fahrer seien ein zentraler Faktor, denn sie können etwa durch unbedachte Äußerungen in der Raststätte Dieben womöglich entscheidende Informationen über Ware und Route verraten.

Vorhandene Sicherheitslösungen an Transportfahrzeugen entsprechen meist nicht den benötigten Erfordernissen, heißt es in der Ausgabe 4-2017 der Zeitschrift Security insight, S. 26. Mit Hilfe der **Geminy Transportersicherung** sei eine einfache Nachrüstung problemlos möglich. Konventionelle Profilzylinder böten zahlreiche Angriffspunkte, da der Zylinder für mögliche Manipulationen immer zugänglich sei. Das Zylinderschutzsystem Geminy beseitige diese Schwachstellen. Auch die patentierte Doppelstifttechnik verhindere unberechtigtes Aufsperren. Einbrecher müssten 22 Mrd. Schließvarianten ausprobieren, ehe sie das System überwinden könnten.

Notruf

Einen **notstromversorgten Sicherheitsrouter für Sprachnotrufe** via IP stellt Security insight in der Ausgabe 4-2017, S. 38, vor. Nach der Umstellung auf All-IP-Netze seien bei einem Stromausfall der Netzzugang und damit auch ein Notruf nicht mehr möglich. Eine Lösung stelle der SIRO-Port N dar. „SIRO" stehe für Sicherheitsrouter, da der SIRO-Port N an allen marktüblichen kupferbasierenden DSL-Anschlüssen einsetzbar sei, über eine Notstromversorgung sowie über ein gehärtetes Betriebssystem verfüge. Gegenüber herkömmlichen GSM-Funklösungen zeichne sich der SIRO-Port N neben Zukunftssicherheit und der Möglichkeit zum Remote-Zugriff durch eine hohe Verfügbarkeit aus. Auch wäre ein Einsatz in Notrufsäulen oder als Altenrufsystem denkbar.

Notruf- und Service-Leitstelle

Ein qualifiziertes Notruf-, Alarm- und Meldungs-Management sei aufwendig und kostenintensiv – wenn man es selber macht, heißt es in sicherheit.info am 1. August. Deshalb würden gerade im gewerblichen Bereich immer mehr Kunden auf **externe NSL** setzen. Ebenso vielfältig wie die ständig wachsenden Gefahren für unser Leben und unsere Infrastruktur seien die Sensoren und Alarmsysteme, die uns rechtzeitig warnen. Was aber häufig vergessen werde: Jeder Notruf und jede Meldung müsse „irgendwo" entgegengenommen werden – und zwar schnell, zuverlässig, qualifiziert, rund um die Uhr, an sieben Tagen in der Woche. Das erfordere eine technische, personelle und organisatorische Infrastruktur, deren Aufbau sich für kleine und mittelständische Unternehmen oft einfach nicht lohne. Die Anforderungen der Sachversicherer, gerade wenn es um vergünstigte Policen geht, seien hoch: So müssten zum Beispiel eingehende Notrufe zu 80 Prozent innerhalb von 30 Sekunden und zu 98,5 Prozent innerhalb einer Minute angenommen werden. Eine Zertifizierung nach DIN 50518 sei aufwendig und teuer. Bei Sensorik, Busstrukturen oder Übertragungsprotokollen gebe es eine Vielzahl von Systemen, vom einfachen Temperaturfühler bis zur komplexen Videoüberwachung. Bei der Reaktion auf die Meldung reiche das Spektrum von der sofortigen Weitergabe eines Alarms an Feuerwehr oder Polizei über die Beauftragung eines Servicetechnikers oder Security-Mitarbeiters bis hin zur Protokollierung von Routinemeldungen.

Auch Sylke Mokrus, Tyco Integrated Fire & Security, befasst sich im Brandschutz Special der Zeitschrift PROTECTOR, Ausgabe 08-2017, S. 30/31, mit dem **NSL-Outsourcing** im gewerblichen Bereich. Weil ein qualifiziertes Notruf-, Alarm- und Meldungs-Management aufwendig und kostenintensiv sei, setzten gerade im gewerblichen Bereich immer mehr Kunden auf externe NSL.

Sicherheitsberater.de weist am 31. August auf seine „**Planungshilfe** für Sicherheitszentralen und Leitstellen" hin: ein Poster im Format DIN A2, das über bestellung@TeMedia-verlag.de bezogen werden könne.

Öffentliche Sicherheit

Den Einsatz **dreidimensionaler Phantombilder für Fahndungszwecke** stellt SecuMedia am 21. Juli vor. Erstmals in Deutschland wende die Polizei in Trier im Fall eines Banküberfalls ein neues dreidimensionales Verfahren an, um Bankräuber zu identifizieren. Die Polizei erhoffe sich dadurch neue Zeugenhinweise zu einem Banküberfall. Zeitgleich stelle sie das neue Verfahren vor, das der Phantombildzeichner des LKA Rheinland-Pfalz, Uwe Kinn, entwickelt habe. Dieses neue Verfahren – die GEMINUS-Datenbank – sei nicht nur weltweit einzigartig. Sie biete den Ermittlern auch bisher nicht gekannte Möglichkeiten, Täter und später Tathandlungen in 3-D darzustellen und auf diese Art weitere Zeugen zu finden. Der Zeuge könne die dargestellte Person aus jeder Perspektive ansehen und das Video derart einstellen, dass es dem Blickwinkel des Zeugen entspricht. Geplant sei auch eine Animation des Täters in einem Ganzkörpermodell in einer Tatort-Attrappe. Auf diese Weise könnten sich Zeugen zukünftig auch eine Rekonstruktion der Tathandlung in dreidimensionaler Ausführung ansehen.

Öffentlicher Personennahverkehr

Im ÖPNV gebe es gute Ansätze für mehr Sicherheit, aber **kein schlüssiges Konzept**, zeigt sich Peter Niggl, Chefredakteur von Security insight, in der Ausgabe 4-2017, S. 13–17, überzeugt. 2016 habe die Deutsche Bahn in Zügen und Bahnhöfen rund 12.500 Gewaltangriffe registriert. Die Zahl der Angriffe auf Sicherheitskräfte, Kontrolleure und andere Mitarbeiter sei in der ersten Hälfte 2016 im Vergleich zum Vorjahreszeitraum bundesweit um 28 Prozent gestiegen, auf rund 1.100 Fälle. Der ÖPNV sei „die Örtlichkeit für Konflikte". Die Bahn habe die Videoüberwachung in den Berliner Bahnhöfen der S-Bahn und der Regionalzüge zuletzt deutlich ausgeweitet. Insgesamt zeichneten 800 Kameras in 100 Bahnhöfen auf, am Bahnhof Südkreuz seien es bislang 80. Die Aufnahmen würden für 48 Stunden gespeichert. Ein Alarmsystem, das die Einleitung von Hilfsmaßnahmen ohne Zeitverzögerung ermögliche, sei jetzt mit dem Projekt „InReakt" von der Studiengesellschaft für Tunnel und Verkehrsanlagen (Stuva) vorgestellt worden. Es soll über eine optische und akustische Sensorik Bewegungsabläufe und Situationen im ÖPNV analysieren und dabei aggressive, auf Tätlichkeiten abzielende Verhaltensmuster erkennen. Bei Einsätzen auf großen Bahnhöfen und zu Sport- und Großveranstaltungen soll das Sicherheitspersonal der Bahn künftig Körperkameras tragen.

Produktpiraterie

Nach einem am 20. Juli veröffentlichten Bericht der Europäischen Kommission haben europäische **Zollbehörden 2016** mehr als 41 Mio. gefälschte Produkte an den Außengrenzen der EU sichergestellt (SecuMedia vom 21. Juli). Das seien zwei Prozent mehr als 2015. Ganz oben auf der Liste der ge-

fälschten Waren stünden nach wie vor Zigaretten (24 Prozent), gefolgt von Spielzeug (17 Prozent), Lebensmitteln (13 Prozent) und Verpackungsmaterial (12 Prozent). Auf Produkte des täglichen Gebrauchs, die die Gesundheit und Sicherheit der Verbraucher gefährden könnten, entfielen zusammen 34,2 Prozent. Auch diesmal sei China mit 80 Prozent aller 2016 beschlagnahmten Waren das Hauptursprungsland nachgeahmter Waren. Aus Vietnam und Pakistan seien erhebliche Mengen an Zigaretten gekommen, aus Singapur nachgeahmte alkoholische Getränke. Bei Fälschungen von Bekleidungszubehör sei Iran Spitzenreiter. Gefälschte Mobiltelefone seien in erster Linie aus Hongkong gekommen, Arzneimittelfälschungen aus Indien.

In der in der August-Ausgabe von Vekoonline vorgestellten Studie „Wirtschaftsmacht OK: illegale Märkte und illegaler Handel" stellt der Autor, Prof. Dr. Arndt Sinn, Universität Osnabrück, **13 konkrete Handlungsempfehlungen** für den Kampf gegen Produktpiraterie und illegalen Handel auf, darunter die Sensibilisierung der Politik für das Thema, personelle Stärkung der Strafverfolgungsbehörden, internationale Joint Investigation Teams, stärkere Kontrolle von Transitstaaten und Freihandelszonen sowie eine bessere Sicherung der Lieferketten durch die Industrie entsprechend den von der Pharma- und Tabakbranche vorgenommenen Maßnahmen. Das Prinzip „know your costumer" müsse zur gelebten Philosophie des Unternehmens gehören.

Rechenzentrumssicherheit

Frank Drolsbach, FM Global, befasst sich im Brandschutz Special der Zeitschrift PROTECTOR, Ausgabe August 2017, S. 14/15, mit dem **Brandschutz in Rechenzentren**. Durch gute Risikomanagementberatung könnten Industriesachversicherer dazu beitragen, Brände in Rechenzentren zu verhindern oder zumindest das Schadensausmaß zu minimieren. Zu den Grundvoraussetzungen gehöre, dass Versorgungsleitungen des Gebäudes für Wasser und Gas nicht durch sensible Bereiche des Serverraumes verlaufen. Laut einer Studie des Ponemon Instituts koste ein Serverausfall ein Unternehmen pro Minute ungefähr 8.000 Euro. Wird ein Brand erkannt, müssten Lüftungsanlagen umgehend abgeschaltet werden, um anliegende Bereiche zu schützen und die Verbreitung von giftigem Rauch über das Belüftungssystem zu stoppen.

Reiserisikomanagement

Die **Rolle des Travel Managers im Notfallmanagement** beleuchtet Pascal Michel, SmartRiskSolutions GmbH, im ASW-Newsletter vom 25. August. Der Travel Manager solle sich fragen: Berücksichtigt die geltende Reiserichtlinie die veränderte Risikolage in Europa? Existiert ein nachhaltiges Reisesicherheitsmanagement? Wie ist vorzugehen, um die Situation eines Reisenden nach einem Terroranschlag zu klären? Wer kann vor Ort helfen? Im Ereignisfall gelte es schnell zu klären: Sind Reisende gegenwärtig in Ereignisnähe zuzuordnen? Kann ich mit ihnen in Kontakt treten? Was empfehle ich Mitarbeitern vor Ort, die weiterhin gefährdet sind? Befinden sich Reisende gerade im Flugzeug auf dem Weg dorthin? Kann ich Mitarbeiter noch vor Reiseantritt erreichen und ggf. stoppen? Wen im Unternehmen muss ich informieren und einbinden?

Schließsystem

Security insight weist in der Ausgabe 4-2017, S. 27, darauf hin, dass die Firmen DB Systel GmbH und Lock Your World GmbH & Co. KG einen „virtuellen Pförtner – **pylocx** – entwickelt haben, ein unabhängiges Schließ-

system mit einem elektronischen Schlüssel: pyKey. Die DB SmartAssist App bestimme, wer zu welchem Zeitpunkt eine Berechtigung zur Ansteuerung des Schlosses erhält. So sei keine physische Verwahrung eines Schließgeheimnisses notwendig. Das System speichere alle Zugänge und mache es möglich, Aufträge transparent zu verfolgen.

Sicherheitsgewerbe

PROTECTOR enthält in der Ausgabe 7/8-2017 eine **Marktübersicht** zu 47 Anbietern von Sicherheitsdiensten. Unter den 66 abgefragten Kriterien befinden sich Fragen nach dem geografischen Geschäftsbereich, nach der Zahl der Mitarbeiter im Sicherheitsbereich und nach der Wahrnehmung von Aufgaben im Objektschutz, im ÖPNV, im Consulting und für JVAs.

Sicherheitstechnik

Auswirkungen der **Digitalisierung in der Sicherheitstechnik** auf die Geschäftsmodelle der Zukunft behandelt Dr. Peter Fey, Dr. Wieselhuber & Partner GmbH, in der Zeitschrift PROTECTOR, Ausgabe 7/8-2017, S. 12/13. Treiber des Megatrends Digitalisierung seien neue Technologien, Vernetzung und Integration, Cyber Security, Datenanalyse und neue Geschäftsmodelle. Gerade im Hinblick auf die öffentliche Sicherheit könnten durch eine gemeinsame Auswertung bisher getrennter „Sicherheitsinseln" in Form von Meta-Netzwerken, schneller und gezielter gefährliche Sachverhalte aufgeklärt werden. Das weite Feld der Data Analytics eröffne den meisten Unternehmen der Sicherheitstechnik wohl die interessantesten Geschäftsperspektiven. Data Analytics bilde einerseits die Grundlage für fundierte sicherheitsrelevante Entscheidungen. Andererseits stelle Data Analytics den Schlüssel zur Identifizierung neuer Geschäftsfelder dar.

Spionage

Elektronische Wellen als Einfallstor für Spionage thematisiert Security insight in der Ausgabe 4-2017, S. 36/37. In der Risikobeurteilung müssten daher neben der IT-K zunehmend auch Wechselwirkungen elektromagnetischer Wellen bzw. deren Abstrahlung einbezogen werden. Wird zum Beispiel ein Gerät mit elektromagnetischen Wellen bestrahlt, könne es passieren, dass die reflektierten Wellen vertrauliche Informationen mit sich führen. Mit dem IoT, Industrie 4.0 oder Logistik 4.0 würden sich Datenübertragungswege wie z. B. NFC, WLAN, Satellit usw. zunehmend drahtlos gestalten. Mit einer patentierten elektromagnetischen Abschirmung im Putz, wahlweise mit Stahlfasern versehen, habe R & A Bau und Bautenschutz in einer Forschungskooperation eine Verfahrensentwicklung zur Absorption und Abschirmung störender elektromagnetischer Wellen auf den Weg gebracht. Die Dimensionierung der Abschirmschicht könne dafür verwendet werden, unerwünschte Frequenzbereiche deutlich mehr zu bekämpfen als den Nutzfrequenzbereich.

Sprachalarmierung

Franziska Becker, TOA Electronics Europe GmbH, befasst sich im Brandschutz Special der Zeitschrift PROTECTOR, Ausgabe 08-2017, S. 38/39, mit der Sprachalarmierung im Brandfall. Nur wenn **BMA und Sprachalarmanlage** eine Einheit bilden, könne die umgehende Evakuierung sichergestellt werden. Es sei erwiesen, dass das Warnen durch eine menschliche Stimme eindeutiger und gleichzeitig beruhigender ist, als ein rein mechanisches Warnsignal. Eine Anwendungsrichtlinie für Errichter und Planer bilde die VDE 0833-4, die unter anderem die Planung sowie den Aufbau und Betrieb für Gefahrenmeldeanla-

gen und die Sprachverständlichkeit innerhalb des Sprachalarmkonzeptes klärt. Die einzelnen Komponenten der Sprachalarmanlage würden als zulässiges Gesamtsystem nach europäischem Standard gelten, wenn die harmonisierten Produktnormen DIN EN 54-4 (Energieversorgungseinrichtungen), DIN EN 54-16 (Sprachalarmzentralen) und DIN EN 54-24 (Lautsprecher) erfüllt sind.

Technische Regelwerke

Den Umgang mit **Abweichungen von technischen Regelwerken** behandelt im Brandschutz Special der Zeitschrift PROTECTOR, Ausgabe 08-2017, S. 9–11, Dipl.-Ing. Matthias Dietrich, Rassek & Partner Brandschutzingenieure. Er geht vor allem auf die Unterschiedlichkeit von Regelungen in den Bundesländern, auf Abweichungen von technischen Regeln, auf die „anerkannten Regeln der Technik" und zivilrechtliche Parameter ein. Sowohl die Listen der „eingeführten technischen Baubestimmungen" als auch die Bauregellisten würden in Zukunft durch die Verwaltungsvorschrift technische Baubestimmung (VVTB) ersetzt. Hier ließen sich künftig die bauordnungsrechtlich verbindlich zu beachtenden technischen Regeln finden. Ergeben sich Abweichungen oder Erleichterungen von verbindlich festgelegten technischen Regeln, so müsse entweder die formale Bestattung einer Abweichung iSd § 67 Abs. 1 Musterbauordnung (MBO) erfolgen oder es sei eine Erleichterung iSd § 51 Abs. 1 MBO darzustellen. Nach der in der DIN EN 45020 vorgegebenen Definition dürften die wenigsten bauaufsichtlich nicht eingeführten technischen Regelwerke uneingeschränkt als „anerkannte Regel der Technik" bezeichnet werden. Ihre Beachtung sei keinesfalls zwingend erforderlich. Abweichungen von technischen Regelwerken könnten unter Umständen dazu führen, dass eine Leistung als mangelhaft anzusehen ist. Abweichungen von technischen Regeln sollten daher grundsätzlich eindeutig und unmissverständlich schriftlich dokumentiert werden.

Terrorismus

Wie Al-Qaida künftig **Anschläge auf Züge** in westlichen Ländern verüben will, beschreibt die FAZ am 31. August. „**Verkehr ist der Schwachpunkt**, auf den wir uns konzentrieren müssen", heiße es in der jüngsten Ausgabe einer Propaganda-Zeitschrift von Al-Qaida. Weil Verkehrsmittel nicht umfassend geschützt werden könnten, seien sie ein besonders lohnendes Ziel von Anschlägen. Weil alle sie benutzten, seien sie ideal, um Angst und das Gefühl der Unsicherheit zu verbreiten. Zudem kosteten Anschläge auf die Verkehrsinfrastruktur die Staaten enorme Summen. Am Beispiel der USA und von Großbritannien zeigten die Terroristen, dass das Bahnnetz höchst verletzbar ist. Und sie empfehlen: Züge könnten direkt von innen oder außen angegriffen werden. Gleise könnten beschädigt oder zerstört werden. Schließlich seien auch die Bahnhöfe ein lohnendes Ziel. Auf zehn Seiten gebe die Zeitschrift eine genaue Anleitung zum Bau eines Werkzeugs, mit dessen Hilfe Züge zum Entgleisen gebracht werden sollten. In der Al-Qaida-Zeitschrift werde eine Karte des Bahnnetzes in den USA veröffentlicht. Doch das BKA warne nun davor, dass auch hierzulande solche Terrorakte möglich seien. Die Gefahr werde von Sicherheitskreisen nicht als höher angesehen als vor der Veröffentlichung der Zeitschrift. Was die Behörden besonders umtreibe, sei die Gefahr eines Anschlags, wie ihn die Terroristen von Barcelona ursprünglich planten – ein großer Anschlag mit einer Autobombe. Für 2016 habe die Bahn 32 Anschläge gezählt, die Linksextreme verübt hätten.

Veranstaltungssicherheit

In der Ausgabe 7/8-2017 der Zeitschrift PROTECTOR wird auf S. 22 der **Veranstaltungsordnungsdienst (VOD)-Mitarbeiter definiert**: Wer als Mitarbeiter eines Bewachungsunternehmens gem. § 34a GewO eine der folgenden Tätigkeiten im Rahmen einer Veranstaltung ohne Übertragung des Hausrechts durch den jeweiligen Veranstalter durchführt und dabei nicht selbstständig handelt, sondern engmaschig durch einen Supervisor/Bereichsleiter geführt wird und nicht einer Erlaubnis nach § 34a GewO bedarf: Kartenabriss, Platzanweisung, Freihalten von Gängen und Fluchtwegen, Kontrolle von Karten und Akkreditierungen, Steuerung von Menschenströmen durch Information, Zufahrtskontrolle, Hilfe bei Evakuierung, Bergen von Hilfsbedürftigen, Lenkung des ruhenden und fließenden Verkehrs im Hausrechtsbereich.

Manfred Buhl, Securitas Deutschland, erläutert in PROTECTOR, Ausgabe 7/8-2017, S. 48–50, das konzeptionelle Vorgehen bei der Planung der Sicherung einer Veranstaltung in zehn Kernpunkten. Und er weist auf den **Optimierungsbedarf im Regelungsbereich** hin: Erlass eines Gesetzes der privaten Sicherheit, das auch für nichtgewerbliche Sicherheitsleistungen gilt; Klarstellung der Entbindung von der Unterrichtung nach § 34a GewO für Ordnungsdienstaufgaben ohne Sicherheitsfunktion; spezifische Zertifizierung als Voraussetzung der Vergabe von Aufgaben der Sicherung einer Veranstaltung.

Sicherheit.info stellt am 15. August die **mobile Antiterror-Barriere Terrablock XL von Betafence** vor. Die Lösung biete hohen Schutz vor Terrorangriffen mit schweren Fahrzeugen und sei dabei optisch ansprechend sowie als Werbefläche nutzbar. Die Wände seien aus einem speziellen Hochsicherheitsgitter gefertigt, in das der Ballastsack eingelassen wird. Das patentierte System sei dafür ausgelegt, beim Anprall eines schweren Fahrzeugs sehr hohe Energien zu absorbieren. Die Anpralllast sei nach internationalem Standard für Fahrzeugbarrieren zertifiziert (IWA 14). Gitter und Ballastsäcke ließen sich flach lagern und transportieren. Vor Ort würden die Gitterwände zusammengebaut. Die einzelnen Terrablock-XL-Module messen 120 mal 120 mal 212 Zentimeter und können ohne Fundamente und ohne Erdarbeiten zu beliebig großen Barrieren kombiniert werden. Auf- und Abbau seien zeitsparend und erforderten weder spezielles Personal noch Schwertransporte.

Rechtliche und regulatorische Anforderungen für **Sicherheitskonzepte von Großveranstaltungen** behandelt Prof. Marcel Kuhlmey in der August-Ausgabe von Veko-online. Es gebe keine grundlegende Vorschrift für die Durchführung von Veranstaltungen oder die Erstellung von Sicherheitskonzepten. Die von vielen Bundesländern übernommene MStättVO beschränke sich auf Versammlungsräume, die mehr als 200 Personen fassen, Veranstaltungsräume im Freien für mehr als 1.000 Besucher und Sportstadien für mehr als 5.000 Personen. Die einzige gesetzliche Regelung, die sich auf Sicherheitskonzepte beziehe, sei § 43 Abs. 1 und 2 MStättVO. Hinzu komme ein Orientierungsrahmen des IM NRW für die kommunale Planung, Genehmigung, Durchführung und Nachbereitung von Großveranstaltungen im Freien. An die Qualifikation des Erstellers eines Sicherheitskonzeptes und für die am Genehmigungsverfahren beteiligten Behörden gebe es keine Anforderungen. In der Praxis würden Sicherheitskonzepte nur dann genehmigt, wenn ein Einvernehmen erzielt werden kann.

Sabine Funk, IBIT GmbH, befasst sich in der August-Ausgabe von Veko-online mit dem privaten **Sicherheits- und Ordnungsdienst bei Veranstaltungen** (VOD). Zu dessen besonderen Herausforderungen zählt die Autorin unregelmäßige Arbeitszeiten, kurzfristige Kräfteanforderungen, unregelmäßige Einsatzorte und damit verbundene Subunter-

nehmerstrukturen. Daraus resultierten u. a. ein hohes Maß an Teilzeitkräften, Aushilfen mit hoher Fluktuation, kaum vorhandene Qualitätssicherungs- und Auswahlprozesse sowie Spannungsfelder zwischen Fürsorgepflichten des Arbeitgebers und Verkehrssicherungspflichten des Auftraggebers. Für die Ordnungskräfte in Fußballstadien habe der DFB ein verbindliches Schulungssystem vorgeschrieben. Für den VOD gebe es keine vergleichbare Vorgabe. Der BDSW habe den VOD definiert und Tätigkeitsbereiche benannt. Im Rahmen des Forschungsprojektes BaSiGo (Bausteine für die Sicherheit von Großveranstaltungen) seien Leistungsmerkmale zusammengefasst worden, die dem Auftraggeber bei der Auswahl des geeigneten VOD behilflich sein können. Dabei handle es sich um die Anforderungen an Erfahrung, Organisationsstruktur, Ausbildung und Entwicklung der Kräfte. Die Autorin listet schließlich Kriterien für die Bemessung der notwendigen Anzahl an Einsatzkräften auf.

Videoüberwachung

Nach einer Meldung von heise.de vom 1. August haben Sicherheitsforscher wieder einmal gravierende **Sicherheitslücken in IP-Kameras** aufgedeckt. Mindestens 175.000 Geräte des Herstellers Shenzhen Neo Electronics ließen sich mit einfachen Mitteln aus dem Netz kapern. Spätestens seit den massiven DDoS-Angriffen des IoT-Botnetzes Mirai sei bekannt, dass solche verwundbaren IP-Kameras beliebte Ziele für Hacker sind, die Bots mit permanenter Internetanbindung für ihre Botnetze rekrutieren wollen. Betroffen seien die Modelle iDoorbell und NIP-22 der NeoCoolCam-Reihe. Es gebe bisher keine Patches.

Die **Energieerzeugung** umfasse viele sicherheitstechnisch sensible Bereiche, die videoüberwacht werden (sicherheit.info am 2. August). Da ein einzelnes Wasserkraftwerk des thailändischen Energieunternehmens Geat bis zu 200 Kameras benötigt, suchte es ein skalierbares und flexibles System. Aufgrund der dezentralen Lage der Anlagen, zu denen auch Staudämme gehören, sei nur eine zentrale und umfassende Lösung in Frage gekommen. Die VMS Xprotect von Milestone integriere alle Kameras der sechs Wasserkraftwerke in ein System.

Andreas Beerbaum und Andreas Conrad, Seetec GmbH, nehmen im Interview Stellung zum **Video-Streaming über 4G- und 5G-Netze** (PROTECTOR, Ausgabe 7/8-2017, S. 23–25). Grundsätzlich eigne sich die bestehende LTE-Technologie bereits seit längerem für die Übertragung von Videoströmen. Die Bandbreiten seien vorhanden, die Abdeckung des Netzes sei gut und werde immer weiter ausgebaut. 5G biete im Vergleich zu heute völlig neue Möglichkeiten in Sachen Bandbreite und Echtzeit-Anwendungen. Das Thema Video, das von Natur aus hohe Bandbreiten beansprucht, andererseits aber gerade im Security-Bereich eine sehr kurze Latenzzeit erfordert, sei dafür prädestiniert. Die Technologie, die für Anwendungen über LTE/5G zum Einsatz komme, heiße „Multi-access Edge Computing" (dezentrale Datenhaltung und -verarbeitung im Gegensatz zum Cloud Computing). Damit bestehe die Möglichkeit, die Videoanwendungen bis auf die Ebene eines Sendemastes oder einer Funkzelle herunter zu brechen. In die Mobilfunk-Infrastruktur einer Zelle seien Serverkomponenten eingebunden, welche die Bildströme von den in der Zelle verteilten Kameras über LTE empfangen, speichern und bei Bedarf mittels Videoanalyse auswerten. Beschließe eine Stadt, die Videoüberwachung auszuweiten, so könne man im bereits bestehenden Mobilfunknetz die Videotechnik betreiben und Analyse- oder Aufzeichnungsfunktionen nutzen.

In der Ausgabe 7/8-2017 von PROTECTOR, S. 28/29, stellt Genetec Deutschland das Sicherheitssystem für das **Olympiastadion**

Lyon vor: Genetec Security Center, zusammen mit der Videoüberwachungslösung Onmicast. Die Sicherheitsplattform Security Center vereine Videoüberwachung, Zutrittskontrolle und Nummernschilderkennung in einer intuitiven Lösung. Omnicast umfasse über 260 Überwachungskameras. Das System ermögliche die Überwachung aller Eingänge, der Gewerbe- und Gastronomiestände, der 7.000 Parkplätze sowie der Zufahrtsstraßen rund um das Olympiaparkstadion. Selbst bei Server- bzw. PC-Fehlern oder sogar bei einem Stromausfall laufe das System aufgrund der redundanten Ausfallsicherung des Security Centers reibungslos weiter. Im nächsten Schritt soll ein Gesichtserkennungssystem in die einheitliche Plattform integriert werden, um Personen mit Stadionverbot zu erkennen.

Dipl.-Phys. Bertrand Völckers, Flir Commercial Vision Systems Deutschland, stellt in der Ausgabe 7/8-2017 der Zeitschrift PROTECTOR, S. 30, das Sicherheitssystem für das **Stadion in Norwich City** vor. Das System VMS Latitude von Flir liefere Bilder in forensischer Qualität und lasse sich über eine komfortable webbasierte und mobile Client-Software bedienen. Zur Videosicherheitslösung gehörten auch verschiedene Hardwarekomponenten, darunter die Kameraserie Quasar von Flir, die mit Quad-HJD-WDR- und 4K-Auflösungen verfügbar ist, kombiniert mit motorisierten Weitwinkel- und Teleobjektiven. Die leistungsstarken Quasar-Modelle böten 76 Prozent mehr Details als Full-HD und den gleichen forensischen Zoom wie die herkömmlichen Fünf-Megapixel-Kameras.

Dipl.-Betriebswirt (FH) Bernd M. Schäfer, Atlas Versicherungsmakler für Sicherheits- und Wertdienste GmbH, weist in der Ausgabe 7/8-2017 von PROTECTOR, S. 31, darauf hin, dass die wenigsten Anbieter von mobiler Sicherheitstechnik gleichzeitig auch Bewachungsunternehmen seien. Damit unterlägen sie nicht der Pflichtversicherung nach § 6 BewachV. Komme es bei einem Nicht-Bewachungsunternehmen zu einem Schadensfall, fehle ein wesentlicher Baustein im Versicherungsschutz.

Sicherheit.info berichtet am 21. August, dass die durch die Direktspeicherarchitektur Trinity unterstützten Wisenet-Kameras die Funktionen eines Networkvideorecorders übernehmen können. In Kombination mit dem sequenziellen Festplattenarchivierungssystem S.F.S. (Sequential disk Filing System) liefere das Speichersystem Coldstore großzügige Speicherkapazitäten zu geringen Kosten. Das System nutze ein Schreibmuster mit gespiegelten, überlappenden Paaren und gewähre so komplette Datenredundanz während des kritischen Schreibvorgangs.

Wirtschaftsschutz

Mehr als die Hälfte der Unternehmen in Deutschland seien in den vergangenen beiden Jahren Opfer von **Wirtschaftsspionage, Sabotage oder Datendiebstahl** geworden, berichtet SecuMedia am 21. Juli als Ergebnis einer Studie von Bitkom, für die 1.069 Geschäftsführer und Sicherheitsverantwortliche quer durch alle Branchen repräsentativ befragt worden seien. Verglichen mit der ersten Studie vor zwei Jahren sei der Anteil von 51 auf 53 Prozent leicht gestiegen, der Schaden zugleich um rund acht Prozent auf 55 Mrd. Euro. In jedem sechsten Unternehmen (17 Prozent) seien in den vergangenen zwei Jahren sensible digitale Daten gestohlen worden, vor allem Kommunikationsdaten (41 Prozent) und Finanzdaten (36 Prozent). In 17 Prozent der Datendiebstähle seien Kundendaten entwendet worden, in elf Prozent Patente oder Informationen aus Forschung und Entwicklung. Häufigstes Delikt sei der Diebstahl von IT- oder Telekommunikationsgeräten. Davon seien 30 Prozent der Unternehmen in den vergangenen zwei Jahren betroffen. Rund jedes fünfte Unternehmen berichte von Social Engineering. Jedes achte Unternehmen sei Opfer von digitaler Sabo-

tage geworden, durch die (auch ehemalige) Mitarbeiter des Unternehmens (62 Prozent). 41 Prozent der betroffenen Unternehmen machten Wettbewerber, Kunden, Lieferanten oder Dienstleister für die Angriffe verantwortlich, 21 Prozent Hobby-Hacker und sieben Prozent organisierte Kriminelle. Der Großteil der Angriffe komme aus dem Ausland: 23 Prozent der Unternehmen berichteten von Tätern aus Osteuropa, 20 Prozent aus China und 18 Prozent aus Russland. Nur 31 Prozent der betroffenen Unternehmen hätte staatliche Stellen eingeschaltet. Eine interne Untersuchung hätten 46 Prozent der Unternehmen eingeleitet. Externe Spezialisten seien von 34 Prozent der Unternehmen hinzugezogen worden. Während alle Unternehmen einen technischen Basisschutz wie etwa Passwörter auf allen Geräten, Firewalls und Virenscanner einsetzten und regelmäßig Backups ihrer Daten anfertigten, seien anspruchsvollere Maßnahmen selten, etwa Intrusion Detection Systeme (20 Prozent) oder Penetrationstests (17 Prozent). Auch im Bereich der organisatorischen Sicherheit seien Standardmaßnahmen weit verbreitet: Festlegung von Zugriffsrechten (99 Prozent), eindeutige Kennzeichnung von Betriebsgeheimnissen (85 Prozent) oder Festlegung von Zutrittsrechten in bestimmte Unternehmensbereiche (81 Prozent). Seltener seien Sicherheits-Zertifizierungen (43 Prozent) oder regelmäßige Sicherheits-Audits durch externe Spezialisten (24 Prozent). Nur jedes zweite Unternehmen habe einen Sicherheitsverantwortlichen benannt (54 Prozent) oder schule seine Mitarbeiter in Sicherheitsfragen (53 Prozent).

„Zugelassener Wirtschaftsbeteiligter (AEO)"

PCS Systemtechnik habe das AEO-Zertifizierungsverfahren erfolgreich durchlaufen und damit den Status des „AEO" erreicht, meldet sicherheit.info am 1. August. Damit sei sichergestellt, dass Luftfrachtgüter unter strengen Sicherheitsmaßnahmen verpackt werden und beschleunigt das Zollverfahren passieren können. Verschiedene organisatorische Maßnahmen seien für den „behördlich anerkannten Bekannten Versender" unabdingbar: So sei zunächst der abzukapselnde Luftfrachtverpackungsbereich zu definieren. Danach müssten bauliche und sicherheitstechnische Maßnahmen wie Überwachung der Türoffenzeiten, Kontrolle von Rolltoren, Lkw-Rampen und anderen Zugängen vorgenommen werden. Die lückenlose Dokumentation aller Zutritte und Türöffnungszeiten, Anwesenheitskontrollen, Festlegung von austrittsüberwachten Raumzonen sowie die regelmäßige Funktionskontrolle des Sicherheitssystems könnten weitere Schutzmaßnahmen sein.

Zutrittskontrolle

Die Zutrittskontrolle bei dem **Arzneimittelhersteller Biotest AG** beschreibt Petra Eisenbeis-Trinkle, Dormakaba, in der Ausgabe 4-2017 der Zeitschrift Security insight, S.23/24. Insgesamt seien über 400 Zugänge im Hauptsitz der Firma online abgesichert. Dazu kämen 660 Zugänge zu Containeranlagen, Büros und Spinden, die mit Offline-Komponenten, c-lever Beschlägen oder Digitalzylindern ausgestattet sind. Hier müssten sich die Mitarbeiter ihre Zutrittsrechte jeden Morgen an einem Update-Terminal neu geben lassen. 1.400 mechanische Schließzylinder seien an Türen zu Technikbereichen verbaut worden.

Das Unternehmen Stabilus, Anbieter von Gasfedern, Dämpfern und elektromechanischen Antrieben, lege den Fokus auf ein **ganzheitliches Zutritts- und Zeitmanagement** und steuere mit einem neuen System von Interflex den Zutritt zum Unternehmen und das Zeitmanagement der Mitarbeiter mithilfe von Firmenausweisen (Security insight,

Ausgabe 4-2017, S. 24/25). Die Türen seien mit elektronischen Beschlägen ausgestattet, die über die NetworkOnCard-Technologie mit dem zentralen System verbunden sind. Im Pförtnergebäude würden Buchungen durchgeführt, bei denen die in der Software verwalteten Zutrittsrechte auf einen Chip des Mitarbeiterausweises geschrieben werden. Jeder Mitarbeiter könne sich damit an den Zutrittspunkten auf dem Weg zu seinem Arbeitsplatz ausweisen.

Sicherheit.info stellt am 24. August Ergebnisse einer aktuellen Studie von Ifsec Global vor, in deren Mittelpunkt die Möglichkeiten und Vorteile stünden, die eine Zutrittskontrollinfrastruktur in Kombination mit vertrauenswürdigen Identitäten für die Vernetzung unterschiedlichster Systeme biete. 60 Prozent der für die Studie Befragten hätten bereits Zutrittskontrollsysteme mit anderen Gebäudemanagementsystemen verknüpft. 51 Prozent der Befragten hätten Zeiterfassungssysteme in andere Gebäudemanagementsysteme integriert, und 45 Prozent sähen Asset-Tracking (Nachverfolgung von Gütern) als den Bereich, der in naher Zukunft am ehesten mit anderen Systemen verknüpft wird. Letztlich deute die ifsec-Global-Untersuchung auch darauf hin, dass die Bedeutung des Internet of Things zunehmen wird.

Impressum

Focus on Security enthält Informationen zum Unternehmensschutz und wird monatlich herausgegeben. Der Focus on Security erscheint per elektronischem Newsletter, der an 1.800 Abonnenten verteilt wird.

Hinweis der Redaktion:
Sämtliche Personenbezeichnungen im Plural gelten auch ohne ausdrückliche Nennung gleichermaßen für männliche und weibliche Personen.

Herausgeber:
Manfred Buhl, Vorsitzender der Geschäftsführung, Düsseldorf

Verantwortlicher Redakteur:
Bernd Weiler, Leiter Kommunikation und Marketing

Beratender Redakteur:
Reinhard Rupprecht, Bonn

focus.securitas.de

Kontakt
Securitas Holding GmbH
Redaktion Focus on Security
Potsdamer Str. 88
D-10785 Berlin

Sitz: Düsseldorf, Amtsgericht Düsseldorf HRB 33348
Geschäftsführer: Manfred Buhl (Vors.), Jens Müller, Gabriele Biesing, Dr. Heiko Kroll
Vorsitzender des Aufsichtsrates: Dr. Carl A. Schade

E-Mail: info@securitas.de